

REMARKS

In response to the Final Office Action mailed March 3, 2008, Applicants respectfully request reconsideration and entry of this amendment. Claims 7 and 11-31 were previously pending in this application. By this amendment, claims 7, 11-13, 19 and 24 have been amended. As a result, claims 7 and 11-31 are pending for examination with claims 7, 19 and 24 being independent. No new matter has been added.

Rejections Under 35U.S.C. §112

The Office Action rejected claims 7, 11-31 under 35 U.S.C. §112. Applicants have amended independent claims 7, 19 and 24 to address the Examiner's concerns.

Accordingly, withdrawal of this rejection is respectfully requested.

Rejections Under 35 U.S.C. §103

The Office Action rejected claims 7-31 under 35 U.S.C. §103(a) as being unpatentable over Terzis, U.S. Published Patent Application No. 2004/0243835 ("Terzis") in view of Lambert, U.S. Published Patent Application No. 2002/0099952 ("Lambert"). Applicants respectfully disagree. In addition, without acceding to the appropriateness of the rejection, Applicants have amended independent claims 7, 19 and 24 to more clearly distinguish over the cited references.

A. Independent Claim 7

Claim 7, as amended, recites:

An object model embodied on a computer-readable medium for managing a service on a computer, the object model comprising:

a policy object model for specifying, by a first user, if it has been determined that the first user is authorized to perform the specification by comparing a rank of the first user against a permitted rank, at least one first policy that the service supports in a packet-centric form, and, by a second user, at least

one second policy by selecting a security level from a plurality of security levels, with each security level from the plurality of security levels being previously set for a specified application and a specified user, *wherein the policy object model comprises a plurality of policy action classes representing at least a deny, permit and log actions of the service on at least one packet*; and

a policy engine platform for interacting of the first user with the at least one first policy and of the second user with the at least one second policy, and to provide the at least one first policy and the at least one second policy to at least one component that performs the service, wherein the policy engine platform comprises a rule editor class that is configured to perform at least one of deleting, adding and editing the at least one first policy by the first user, and a setting editor class that is configured to enable the second user to select the security level from the plurality of security levels.

(Emphasis added).

Claim 7 has been amended to recite, inter alia, “wherein the policy object model comprises a plurality of policy action classes representing at least a deny, permit and log actions of the service on at least one packet” Support for this amendment can be found, for example, on page 18, ¶ 0041, page 24, ¶ 0048 and on pages 70-72 (Exhibit C) of the present specification.

Terzis discusses resource access rules 675 that are used to control which users have access to what resources. (Terzis, page 9, ¶ 0120). The resource access rules define priority, source, resource, permission level, allowable identifiers, denied identifiers, log type, active time, peer type and peer. (Terzis, page 9, ¶ 0120). In the case of L4 resources, the permission level can be accept, drop, or deny. (Terzis, page 9, ¶ 0121). Terzis also describes that the local execution 625 object contains the actions that will be performed for requests that match the filters in a content rule. (Terzis, page 8, ¶ 0110). The local execution 625 includes service name (of services to be executed) and service parameters. (Terzis, page 8, ¶ 0110). The filter field references the name of a content filter element object that already exists in a policy database and the action field defines the local executions that can be performed. (Terzis, page 10, ¶ 0129). The local executions include but are not limited to, EXEC_FORWARD (forward client requests from one MACSS to the other and are created automatically) and EXEC_DROP (implement the signature matching function that is part of application level security). (Terzis, page 10, ¶ 0129).

Nowhere does Terzis describe a plurality of *policy action classes* representing at least a deny, permit and log actions of the service on at least one packet, as recited in claim 7.

Similarly, Lambert does not teach or suggest a plurality of policy action classes representing at least a deny, permit and log actions of the service on at least one packet.

In view of the above, neither Terzis nor Lambert teaches or suggests “wherein the policy object model comprises a plurality of policy action classes representing at least a deny, permit and log actions of the service on at least one packet,” as recited in claim 7.

In view of the foregoing, claim 7 patentably distinguishes over Terzis and Lambert, either alone or in combination.

Claims 11-18 depend from claim 7 and are allowable for at least the same reasons.

Therefore withdrawal of the rejection of claims 7 and 11-18 is respectfully requested.

B. Independent Claim 19

Claim 19, as amended, recites:

A method of managing a service on a computer, the method comprising:
specifying, via a policy object model, by a first user, if it has been determined that the first user is authorized to perform the specification by comparing a rank of the first user against a permitted rank, at least one first policy that the service supports in a packet-centric form, and, by a second user, at least one second policy by selecting a security level from a plurality of security levels, with each security level from the plurality of security levels being previously set for a specified application and a specified user, *wherein the policy object model comprises a plurality of policy action classes representing at least a deny, permit and log actions of the service on at least one packet;*

interacting, via a policy engine platform, of the first user with the at least one first policy, and of the second user with the at least one second policy; and

providing, via the policy engine platform, the at least one first policy and the at least one second policy to at least one component that performs the service, wherein the policy engine platform comprises a rule editor class that is configured to perform at least one of deleting, adding and editing the at least one first policy by the first user, and a setting editor class that is configured to enable the second user to select a security level from the plurality of security levels.

(Emphasis added).

Claim 19 has been amended to recite, inter alia, “wherein the policy object model comprises a plurality of policy action classes representing at least a deny, permit and log actions of the service on at least one packet” Support for this amendment can be found, for example, on page 18, ¶ 0041, page 24, ¶ 0048 and on pages 70-72 (Exhibit C) of the present specification.

As discussed above, neither Terzis nor Lambert teaches or suggests that “wherein the policy object model comprises a plurality of policy action classes representing at least a deny, permit and log actions of the service on at least one packet,” as recited in claim 19.

In view of the foregoing, claim 19 patentably distinguishes over Terzis and Lambert, either alone or in combination.

Claims 20-23 depend from claim 19 and are allowable for at least the same reasons.

Therefore withdrawal of the rejection of claims 19-23 is respectfully requested.

C. Independent Claim 24

Claim 24, as amended, recites:

An object model embodied on a computer-readable medium for managing a firewall service on a computer, the object model comprising:

a policy object model used to specify, by a first user, if it has been determined that the first user is authorized to perform the specification by comparing a rank of the first user against a permitted rank, at least one first policy that the firewall service supports in a packet-centric form, and, by a second user, at least one second policy by selecting a security level from a plurality of security levels, with each security level from the plurality of security levels being previously set for a specified application and a specified user, the policy object model comprising a policyrule object usable to generate a policy, the policyrule object comprising a condition property and an action property, wherein the policy generated by the policyrule object is configured to perform an action specified in the action property responsive to a condition specified in the condition property being met, *wherein the policy object model comprises a plurality of policy action classes representing at least a deny, permit and log actions of the firewall service on at least one packet*; and

a policy engine platform comprising a rule editor class that is configured to perform at least one of deleting, adding and editing the at least one first policy by the first user, and a setting editor class that is configured to enable the second user to select a security level from the plurality of security levels.

(Emphasis added).

Claim 24 has been amended to recite, inter alia, “wherein the policy object model comprises a plurality of policy action classes representing at least a deny, permit and log actions of the service on at least one packet” Support for this amendment can be found, for example, on page 18, ¶ 0041, page 24, ¶ 0048 and on pages 70-72 (Exhibit C) of the present specification.

As discussed above, neither Terzis nor Lambert teaches or suggests that “wherein the policy object model comprises a plurality of policy action classes representing at least a deny, permit and log actions of the service on at least one packet,” as recited in claim 24.

In view of the foregoing, claim 24 patentably distinguishes over Terzis and Lambert, either alone or in combination.

Claims 25-31 depend from claim 24 and are allowable for at least the same reasons.

Therefore withdrawal of the rejection of claims 24-31 is respectfully requested.

CONCLUSION

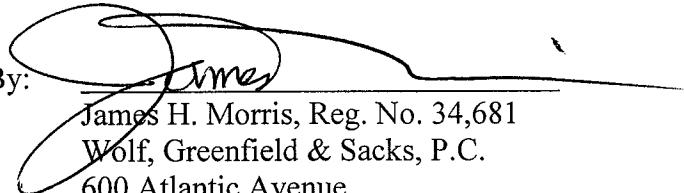
A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: May 2, 2008

Respectfully submitted,

By:



James H. Morris, Reg. No. 34,681
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
Telephone: (617) 646-8000